B. AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computer-implemented method for securing data, said method comprising:
receiving, at a security module, a first password corresponding to a software application;
generating, at the security module, a first mask value based on the first password;
combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;
returning the encrypted tied key to the software application;
determining, at the software application, that the encrypted tied key corresponds to the security module;
in response to the determining, sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password;
receiving, at the security module, the encrypted tied key and the second password from the software application;
in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key;
~~receiving a second password corresponding to the software application;~~

generating a second mask value based on the second password;
separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and
encrypting data provided by the software application using the recovered generated key.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Currently Amended) The computer-implemented method as described in claim 1 further comprising:
determining whether the recovered known value is correct; and
processing a data file based on the determination.

7. (Currently Amended) The computer-implemented method as described in claim 6 wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key.

8. (Currently Amended) An information handling system comprising:
one or more processors;
a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a hardware security module accessible by the processors;

a data security tool for securing data using the hardware security module, the data security tool including:

means for receiving, at a security module, a first password corresponding to a software application;

means for generating, at the security module, a first mask value based on the first password using the hardware security module;

means for combining, at the security module, the first mask value with a first encryption key using the hardware security module, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;

means for encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;

means for returning the encrypted tied key to the software application;

means for determining, at the software application, that the encrypted tied key corresponds to the security module;

in response to the determining, sending the encrypted tied key and a second password from the software application to the security module, the second password being the same as the first password;

means for receiving, at the security module, the encrypted tied key and the second password from the software application;

means for, in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key;

~~means for receiving a second password corresponding to the software application;~~

means for generating a second mask value based on the second password using the hardware security module;

means for separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

means for encrypting data provided by the software application using the recovered generated key.

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Original) The information handling system as described in claim 12 wherein the means for processing is selected from the group consisting of a means for encrypting the data file using the recovered generated key and a means for decrypting the data file using the recovered generated key.

14. (Currently Amended) A computer program product stored in a computer operable media for securing data, said computer program product comprising:

means for receiving, at a security module, a first password corresponding to a software application;
means for generating, at the security module, a first mask value based on the first password using the hardware security module;
means for combining, at the security module, the first mask value with a first encryption key using the hardware security module, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
means for encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;
means for returning the encrypted tied key to the software application;
means for determining, at the software application, that the encrypted tied key corresponds to the security module;
in response to the determining, sending the encrypted tied key and a second password from the software application to the security module, the second password being the same as the first password;
means for receiving, at the security module, the encrypted tied key and the second password from the software application;
means for, in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key;
~~means for receiving a second password corresponding to the software application;~~

means for generating a second mask value based on the second password using the hardware security module;
means for separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and
means for encrypting data provided by the software application using the recovered generated key.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Original) The computer program product as described in claim 14 further comprising:
means for determining whether the recovered known value is correct; and
means for processing a data file corresponding to the determination.

20. (Original) The computer program product as described in claim 19 wherein the means for processing is selected from the group consisting of a means for encrypting the data file using the recovered generated key and a means for decrypting the data file using the recovered generated key.

21. (New) The method of claim 1 wherein the security module is a separate hardware security module in a computer system.

22. (New) The method of claim 1 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

23. (New) The method of claim 1 wherein encrypting the data is performed within the security module.

24. (New) The information handling system of claim 8 wherein the security module is a separate hardware security module in a computer system.

25. (New) The information handling system of claim 8 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

26. (New) The information handling system of claim 8 wherein encrypting the data is performed within the security module.

27. (New) The computer program product of claim 14 wherein the security module is a separate hardware security module in a computer system.

28. (New) The computer program product of claim 14 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

29. (New) The computer program product of claim 14 wherein encrypting the data is performed within the security module.